IN THE UNITED STATES DISTRICT COURT
DISTRICT OF NEBRASKA

JERRY GIBBONS, individually and on behalf of all others similarly situated, Plaintiff, v. **REGIONAL CARE, INC.,** Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff JERRY GIBBONS, as an individual and on behalf of the Class defined below of similarly-situated persons (collectively, "Plaintiff and Class Members"), alleges the following against Defendant Regional Care, Inc., ("Defendant" or "RCI"). The following allegations are based on Plaintiff's knowledge, investigations by Plaintiff's counsel, facts of public record, and information and belief:

NATURE OF THE ACTION

1. Plaintiff seeks to hold Defendant responsible for the injuries it inflicted on Plaintiff and others due to Defendant's inadequate data security, which resulted in the sensitive personal data of Plaintiff and those similarly situated to be exposed to unauthorized third parties (the "Data Breach").

2. RCI is a third-party health plan administrator that works with more than 25,000 members across Nebraska and nationwide.[1]

3. The data that Defendant exposed to the public is unique and highly sensitive. For one, the exposed data included personal identifying information ("PII") and protected health

[1] Regional Care, Inc., *The RCI Story*, https://www.regionalcare.com/history (last visited Dec. 23, 2024).

information ("PHI") like full names, Social Security numbers, dates of birth, genders, health insurance information, and medical information, which Plaintiff and Class Members provided to Defendant with the understanding Defendant would keep that information private in accordance with both state and federal laws.

4. On September 18, 2024, RCI detected unusual activity on its internal computer network. As a result, the security and privacy of the Private Information of Defendant's clients and employees was impacted.

5. Among myriad industry standards and statutes for protection of sensitive information, PHI is specifically governed by federal law under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations. HIPAA requires entities like RCI to take appropriate technical, physical, and administrative safeguards to secure the privacy of PHI, establishes national standards to protect PHI, and requires timely notice of a breach of unencrypted PHI.

6. Instead of following these rules, however, RCI disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to implement reasonable measures to safeguard Private Information and by failing to take necessary steps to prevent unauthorized disclosure of that information. RCI's woefully inadequate data security measures made the Data Breach a foreseeable, and even likely, consequence of its negligence.

7. Exacerbating the injuries to Plaintiff and Class Members, RCI failed to provide timely notice to Plaintiff and Class Members, depriving them of the chance to take speedy measures to protect themselves and mitigate harm. When RCI finally did notify Plaintiff and Class Members of the disclosure, it offered no assurances that all personal data or copies of data have been recovered or destroyed, or that RCI has adequately enhanced its security practices or

dedicated sufficient resources and staff to avoid a breach of its network in the future.

8. Today, the PII and PHI of Plaintiff and Class Members continue to be in jeopardy because of Defendant's actions and inactions described herein. Plaintiff and Class Members now suffer from a heightened and imminent risk of fraud and identity theft for years to come and now must constantly monitor their medical and financial accounts for unauthorized activity.

9. The PII and PHI (collectively "Private Information") exposed in the Data Breach can enable criminals to commit a litany of crimes. Criminals can open new financial accounts in Class Members' names, take out loans using Class Members' identities, use Class Members' names to obtain medical services, use Class Members' health information to craft phishing and other hacking attacks based on Class Members' individual health needs, use Class Members' identities to obtain government benefits, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names (but with another person's photograph), and give false information to police during an arrest.

10. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have suffered actual and present injuries, including but not limited to: (a) present, certainly impending, and continuing threats of identity theft crimes, fraud, scams, and other misuses of their Private Information; (b) diminution of value of their Private Information; (c) loss of benefit of the bargain (price premium damages); (d) loss of value of privacy and confidentiality of the stolen Private Information; (e) illegal sales of the compromised Private Information; (f) mitigation expenses and time spent responding to and remedying the effects of the Data Breach; (g) identity theft insurance costs; (h) "out of pocket" costs incurred due to actual identity theft; (i) credit freezes/unfreezes; (j) anxiety, annoyance, and nuisance; (k) continued risk to their Private Information, which remains in RCI's possession and is subject to further breaches so long as RCI

fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information; and (l) disgorgement damages associated with RCI's maintenance and use of Plaintiff's and Class Members' data for its benefit and profit.

11. Through this action, Plaintiff seeks to remedy these injuries on behalf of himself and all similarly situated individuals whose Private Information was exposed and compromised in the Data Breach.

12. Plaintiff brings this action against RCI and assert claims for negligence, negligence *per se*, unjust enrichment, breach of implied contract, and injunctive relief.

PARTIES

13. Plaintiff Jerry Gibbons is a natural person, resident, and citizen of Nebraska, residing in Scotts Bluff County.

14. Defendant Regional Care, Inc., is a Nebraska corporation with its principal place of business at 905 West 27th Street, Scottsbluff, Nebraska 69361.

JURISDICTION AND VENUE

15. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. And minimal diversity is established because Plaintiff (and many members of the Nationwide Class) are citizens of states different than Defendant.

16. This Court has general personal jurisdiction over Defendant because Defendant is a corporation incorporated under the laws of Nebraska, and whose principal place of business is in Scottsbluff, Nebraska. Defendant also regularly conducts substantial business in Nebraska.

17. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because substantial part of the events giving rise to the claims emanated from activities

within this District, and Defendant conducts substantial business in this District.

FACTUAL ALLEGATIONS

Defendant Collected and Stored the Private Information of Plaintiff and Class Members

18. RCI is a corporation that offers health plan administration services to its clients and broker partners.[2]

19. Plaintiff and Class Members provided their Private Information either directly or indirectly through Defendant's clients and/or broker partners to RCI in exchange for their health plan management services.

20. Upon information and belief, Defendant would collect and does collect from Plaintiff and Class Members the following types of Private Information, including but not limited to: full names, Social Security numbers, dates of birth, gender, health insurance information, and medical information.

21. Upon information and belief, this Private Information is then stored on Defendant's computer network.

22. Because of the highly sensitive and personal nature of the information Defendant acquires and stores, Defendant knew or reasonably should have known that it must comply with healthcare industry standards related to data security and all federal and state laws protecting Private Information and provide adequate notice if Private Information is disclosed without proper authorization.

23. Indeed, Defendant both explicitly and implicitly promised Plaintiff and Class Members that it used reasonable measures to safeguard the Private Information it collects from theft and misuse.

[2] Regional Care, Inc., *About Regional Care, Inc.*, https://www.regionalcare.com/about (last visited Dec. 23, 2024).

24. Plaintiff and Class Members provided their Private Information to RCI as a condition of receiving products and services from RCI, but in doing so, expected RCI to keep the Private Information confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

The Data Breach

25. On or after December 16, 2024, RCI began sending Plaintiff and Class Members a notification letter ("Notice of Data Breach"). Defendant also posted a notice to its website, stating as follows:

> The privacy and security of the personal information we maintain is of the utmost importance to Regional Care, Inc. ("RCI").
>
> On or about September 18 2024, RCI detected unusual activity on an account on its network and determined an unauthorized party potentially accessed and/or acquired a limited number of files from our computer systems. Upon discovery, we immediately shut down the account, contained the incident and commenced an immediate and thorough investigation. As part of our investigation, we engaged leading cybersecurity experts to identify what personal information, if any, was involved.
>
> After an extensive forensic investigation and manual document review, we concluded on or about November 8, 2024 that one or more of the files potentially accessed and/or acquired by the unauthorized party contained some sensitive personal information. The potentially impacted information varies by individual, and may include the impacted individual's full name, dates of birth, Social Security number, medical information, and health insurance information.
>
> Out of an abundance of caution, commencing on December 16, 2024, RCI notified individuals whose information may have been included in the files accessed by the unauthorized party. Notified individuals have been provided with best practices to protect their information, and individuals whose Social Security numbers were contained in the impacted files have been offered complimentary credit monitoring.
>
> RCI is committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. RCI continually evaluates and modifies its practices and internal controls to enhance the security

and privacy of your personal information.[3]

26. Upon information and belief, Plaintiff's and Class Members' affected Private Information at the time of the Data Breach were accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by unauthorized individuals.

27. The notice posted to the website for all Defendant's customers and clients reflects that language sent to Plaintiff in the Notice of Data Breach letter that he received, attached as **Exhibit 1** hereto.

28. Both statements from Defendant claim that "[t]he privacy and security of the personal information [Defendant] maintain[s] is of the utmost importance to Regional Care, Inc." And each statement acknowledges the severity of the Data Breach by providing instructions for how the victims can try to protect themselves from the Data Breach, including instructions on how to place fraud alerts on credit, encouragement to freeze credit files, and an assertion that victims "should remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis."[4]

29. Upon information and belief, as a result of the Data Breach, unauthorized individuals obtained access to and stole the following types of Private Information about Plaintiff and Class Members stored on Defendant's IT systems: full names, Social Security numbers, dates of birth, genders, health insurance information, and medical information.

30. Upon information and belief, Defendant was a target due to its status as healthcare-related entity that collects, creates, and maintains Private Information.

---

[3] *Regional Care, Inc. Notifies Customers and Clients of Data Security Incident* (Dec. 16, 2024), https://www.regionalcare.com/_files/ugd/08cced_e2e1b5bf773f46c5af66062f13ade51b.pdf (last visited Dec. 23, 2024).

[4] *Id*; Ex. 1, Notice of Data Breach Letter.

31. Time is of the essence when highly sensitive Private Information is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired Private Information of Plaintiff and Class Members is now likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted Private Information to criminals.

32. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their Private Information, especially their Social Security numbers and sensitive medical information, onto the Dark Web. Plaintiff and Class Members face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing hundreds of thousands of Social Security numbers and/or specific, sensitive medical information.

33. RCI largely put the burden on Plaintiff and Class Members to take measures to protect themselves from identity theft and fraud.

34. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.6% of U.S.-based workers are compensated on an hourly basis, while the other 44.4% are salaried.[5]

35. According to the American Time Use Survey, American adults have between 4 to 6 hours of "leisure time" outside of work per day;[6] examples of leisure time include partaking in

[5] U.S. Bureau of Labor Statistics, *Characteristics of minimum wage workers, 2022* (Aug. 2023), https://www.bls.gov/opub/reports/minimum-wage/2022/home.htm#:~:text=The%20following%20are%20highlights%20from,federal%20minimum%20wage%20or%20less (last visited Dec. 23, 2024).

[6] Eric Snodgrass, *Americans have no idea how to use their free time*, Business Insider (Mar. 26, 2024), https://www.businessinsider.com/americans-free-time-leisure-dont-use-television-2024-3#:~:text=Americans%2C%20on%20average%2C%20have%20between,people%20spend%20doing%20various%20activities (last visited Dec. 23, 2024).

sports, exercise and recreation; socializing and communicating; watching TV; reading; thinking/relaxing; playing games and computer use for leisure; and other leisure activities.[7] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

36. Plaintiff and Class Members are deprived of the choice as to how to spend their valuable free hours and therefore seek renumeration for the loss of valuable time as another element of damages.

37. As another element of damages, Plaintiff and Class Members seek a sum of money sufficient to provide to Plaintiff and Class Members identity theft protection services for their respective lifetimes.

38. In response to this Data Breach, Defendant offered some of the victims one year of non-automatic single bureau credit monitoring, which is dramatically insufficient to provide meaningful protection to the Class Members, but which is also a tacet acknowledgment of the imminent risk of future harm now faced by Plaintiff and Class Members.[8]

39. Plaintiff and the Class Members remain in the dark regarding exactly what data was stolen, the particular method of disclosure, the results of any investigations, and what steps are being taken, if any, to secure their Private Information going forward. Plaintiff and Class Members are left to speculate as to the full impact of the Data Breach and how exactly

[7] U.S. Bureau of Labor Statistics, *Table 11A. Time spent in leisure and sports activities for the civilian population by selected characteristics, averages per day, 2022 annual averages* (June 27, 2023), https://www.bls.gov/news.release/atus.t11A.htm (last visited December 23, 2024).

[8] Ex. 1, Notice of Data Breach letter.

Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

40. RCI could have prevented the Data Breach by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiff's and Class Members' Private Information.

41. Defendant's negligence in safeguarding Plaintiff's and Class Members' PII and PHI was exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

42. Healthcare organizations have become a main target for cybercriminals because they "hold a massive amount of patient data — including medical records, financial information, Social Security numbers, names and addresses. They're also among the few businesses that stay open 24/7, meaning they might be more likely to prioritize avoiding disruptions and, therefore, more likely to pay a hacker's ransom."[9]

43. In the context of data breaches, healthcare is "by far the most affected industry sector."[10] Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.[11]

44. Despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff's and

[9] Elise Takahama, *Why health care has become a top target for cybercriminals*, The Seattle Times (Feb. 25, 2024), https://www.seattletimes.com/seattle-news/health/why-health-care-has-become-a-top-target-for-cybercriminals (last visited December 23, 2024).

[10] Rody Quinlan, *Healthcare Security: Ransomware Plays a Prominent Role in COVID-19 Era Breaches*, Tenable (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last visited December 23, 2024).

[11] *See id.*

Class Members' Private Information from being compromised.

45. RCI failed to properly train its employees as to cybersecurity best practices and to maintain proper staffing and processes for responding to and preventing network intrusions.

46. RCI failed to implement sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions.

47. RCI failed to encrypt Plaintiff's and Class Members' Private Information and monitor user behavior and activity to identify possible threats.

48. RCI failed to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

49. RCI failed to timely and accurately disclose that Plaintiff's and Class Members' PII and PHI had been improperly acquired or accessed.

50. RCI knowingly disregarded standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured PII and PHI.

Defendant Failed to Comply with FTC Guidelines

51. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[12] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII and PHI.

52. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices

[12] Fed. Trade Comm'n, *Start With Security, A Guide for Business: Lessons Learned From FTC Cases*, (Aug. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf (last visited Dec. 23, 2024).

for business.[13] The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

53. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

54. The FTC recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[14]

55. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

56. These FTC enforcement actions include actions against healthcare providers and

[13] Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Dec. 23, 2024).

[14] *Start with Security*, *supra*, https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf.

partners like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

57. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

58. Despite its alleged commitments to securing sensitive data, RCI does not follow industry standard practices in securing Private Information.

59. As shown above, experts studying cyber security routinely identify healthcare related entities as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

60. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Defendant, including but not limited to, educating all employees on the risks of cyber attacks; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

61. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems;

protection against any possible communication system; training staff regarding critical points.

62. Upon information and belief, RCI failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

63. Such frameworks are the existing and applicable industry standards in the healthcare industry. And RCI failed to comply with these accepted standards, thus opening the door to criminals and the Data Breach.

Defendant Violated HIPAA and HITECH

64. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[15]

65. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[16]

66. The Data Breach itself resulted from a combination of inadequacies showing

[15] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[16] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §

164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

67. RCI is also required to follow the regulations for safeguarding electronic medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

68. Both HIPAA and HITECH obligate RCI to follow reasonable security standards, respond to, contain, and mitigate security violations, and to protect against disclosure of sensitive Private Information. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); 45 C.F.R. § 164.530(f); 42 U.S.C. § 17902.

Plaintiff 's Experiences and Injuries Caused by the Data Breach

69. Plaintiff and Class Members are current/former participants of health plans serviced by RCI or current/former employees of RCI.

70. As a prerequisite of receiving medical services from RCI, Defendant required Plaintiff and Class Members to provide their Private Information.

71. RCI began notifying Plaintiff and Class Members about the Data Breach on or around May 2024.

72. When RCI finally announced the Data Breach, it deliberately underplayed the

severity and obfuscated the nature of the Data Breach. Defendant's cybersecurity event update on its website fails to adequately explain how the breach occurred, what exact data elements of each affected individual were compromised, and the extent to which those data elements were compromised.

73. Because of the Data Breach, Defendant inflicted injuries upon Plaintiff and Class Members. And yet, Defendant has done little to provide Plaintiff and the Class Members with relief for the damages they suffered.

Plaintiff Jerry Gibbons

74. Plaintiff Jerry Gibbons is an adult individual and a natural person of Missouri, where he intends to stay.

75. RCI obtained Plaintiff's Private Information because Plaintiff, as a client of RCI, was required to give his information to RCI to obtain Defendant's health plan management services and, through Defendant, healthcare services in general.

76. Upon information and belief, Defendant maintained Plaintiff's Private Information at the time of the Data Breach.

77. On or about December 16, 2024 Plaintiff Gibbons received a Notice of Data Breach letter from RCI informing Plaintiff that his Private Information may have been compromised in the Data Breach.

78. Plaintiff is a reasonably cautious person and is therefore careful about sharing any sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive information over the internet or any other unsecured source. Plaintiff stores any documents containing sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online

accounts, changing and refreshing them as needed to ensure their respective various information is as protected as it can be. When it is available, Plaintiff use two-factor or multifactor authentication to add an extra layer of security to Private Information.

79. Plaintiff only allowed Defendant to maintain, store, and use Plaintiff 's Private Information because he believed that Defendant would use basic security measures to protect Plaintiff 's Private Information, such as requiring passwords and multi-factor authentication to access databases storing the Private Information. As a result, Plaintiff 's Private Information was within the possession and control of Defendant at the time of the Data Breach.

80. In the instant that Plaintiff's Private Information was accessed and obtained by a third party without Plaintiff's consent or authorization, Plaintiff suffered injury from a loss of privacy.

81. Plaintiff has been further injured by the damages to and diminution in value of Plaintiff's Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when Plaintiff 's Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

82. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from Plaintiff 's Private Information being placed in the hands of criminals.

83. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, and self-monitoring Plaintiff 's accounts and credit reports and those of Plaintiff to ensure no fraudulent activity has

occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

84. The substantial risk of imminent harm and loss of privacy have caused Plaintiff to suffer stress, fear, and anxiety. Plaintiff has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff and the Class Face Significant Risk of Present and Continuing Identity Theft

85. Plaintiff and Class Members suffered injury from the misuse of their PII and PHI that can be directly traced to Defendant.

86. The ramifications of Defendant's failure to keep Plaintiff 's and the Class's PII and PHI secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

87. In 2021, 32% of persons age 16 or older who received breach notification were victims of multiple types of identity theft.[17]

88. As a result of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiff and Class Members suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII and PHI is used;

[17] Erika Harrell, PhD, *Data Breach Notifications and Identity Theft, 2021*, U.S. Bureau of Justice Statistics (Jan. 2024), https://bjs.ojp.gov/data-breach-notifications-and-identity-theft-2021 (last visited Dec. 23, 2024).

b. The diminution in value of their PII and PHI;

c. The compromise and continuing publication of their PII and PHI;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII and PHI; and

h. The continued risk to their PII and PHI, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII and PHI in their possession.

89. Stolen PII and PHI is one of the most valuable commodities on the criminal information black market. According to Prey, a company that develops device tracking and recovery software, stolen PII and PHI can be worth up to $2,000.00 depending on the type of information obtained.[18]

90. The value of Plaintiff 's and the Class's Private Information on the black market is considerable. Stolen PII and PHI trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites,

[18] Juan C. Hernandez, *Dark web: lifecycle of stolen credentials explored*, Prey (Feb. 26, 2024), https://preyproject.com/blog/lifecycle-stolen-credentials-dark-web (last visited Dec. 23, 2024).

making the information publicly available, for a substantial fee of course.

91. It can take victims years to spot or identify PII and PHI theft, giving criminals plenty of time to milk that information for cash.

92. One such example of criminals using PII and PHI for profit is the development of "Fullz" packages.[19]

93. Cyber-criminals can cross-reference two sources of PII and PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

94. The development of "Fullz" packages means that stolen PII and PHI from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII and PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members

[19] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/tag/fullz/ (last visited Dec. 23, 2024).

of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff 's and other members of the proposed Class's stolen PII and PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

95. According to the FBI's Internet Crime Complaint Center (IC3) 2023 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $12.5 billion in losses to individuals and business victims.[20]

96. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

97. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII and PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

98. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[21]

---

[20] Fed. Bureau of Investigation, *Internet Crime Report 2023*, https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf (last visited Dec. 23, 2024).

[21] Pamela J. Harbour, *Remarks Before FTC Exploring Privacy Roundtable* (Fed. Trade Comm'n, Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited Dec. 23, 2024).

99. The FTC has issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.[22] According to the FTC, data security requires: (1) controlling access to data sensibly; (2) requiring secure passwords and authentication; (3) storing sensitive information securely and protecting it during transmission; (4) segmenting networks and monitoring who is trying to get in and out; (5) securing remote access to networks; (6) applying sound security practices when developing new products; (7) ensuring that third-party service providers implement reasonable security measures; (8) putting in place procedures to keep security current and address potential vulnerabilities; and (9) securing paper, physical media, and devices.[23]

100. According to the FTC, unauthorized PII and PHI disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout.[24] The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act (the "FTCA").

101. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ⁋ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system

[22] *Start With Security*, *supra*, https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf.

[23] *Id.*

[24] *See* Fed. Trade Comm'n, *Taking Charge, What to Do if Your Identity is Stolen*, at 3 (Jan. 2012), NCJRS Virtual Library, https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen (last visited Dec. 23, 2024).

logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations. Defendant thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of PII and PHI.

102. Healthcare organizations have become a main target for cybercriminals because they "hold a massive amount of patient data — including medical records, financial information, Social Security numbers, names and addresses. They're also among the few businesses that stay open 24/7, meaning they might be more likely to prioritize avoiding disruptions and, therefore, more likely to pay a hacker's ransom."[25]

103. Charged with handling highly sensitive PII and PHI including healthcare information, financial information, and insurance information, Defendant knew or should have known the importance of safeguarding the PII and PHI that was entrusted to it. Defendant also knew or should have known of the foreseeable consequences if its data security systems were

[25] Takahama, *supra*, https://www.seattletimes.com/seattle-news/health/why-health-care-has-become-a-top-target-for-cybercriminals/.

breached. Defendant nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

104. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PII and PHI of Plaintiff and Class Members to unscrupulous operators, con artists, and outright criminals.

CLASS ACTION ALLEGATIONS

105. Plaintiff brings this class action on behalf of all members of the following Class of similarly situated persons pursuant to Federal Rule of Civil Procedure 23. Plaintiff seeks certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3) of the following Nationwide Class (the "Class"):

Nationwide Class

All persons residing in the United States whose Private Information was impacted by the Data Breach disclosed by Defendant in or about May 2024 (the "Class").

106. The Class defined above is readily ascertainable from information in Defendant's possession. Thus, such identification of Class Members will be reliable and administratively feasible.

107. Excluded from the Class are: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or their parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and

Defendant's counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

108. Plaintiff reserves the right to amend or modify the Class definitions as this case progresses.

109. Plaintiff satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

110. **Numerosity**. Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of thousands of individuals whose PII and PHI were compromised by Defendant's Data Breach.

111. **Commonality**. There are many questions of law and fact common to the Class. And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, without limitation:

a. If Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII and PHI;

b. If Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. If Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, HIPAA;

d. If Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. If Defendant owed a duty to Class Members to safeguard their PII and PHI;

f. If Defendant breached its duty to Class Members to safeguard their PII and PHI;

g. If Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. If Defendant should have discovered the Data Breach earlier;

i. If Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

j. If Defendant's delay in informing Plaintiff and Class Members of the Data Breach was unreasonable;

k. If Defendant's method of informing Plaintiff and Class Members of the Data Breach was unreasonable;

l. If Defendant's conduct was negligent;

m. If Plaintiff and Class Members were injured as a proximate cause or result of the Data Breach;

n. If Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

o. If Defendant breached implied contracts with Plaintiff and Class Members;

p. If Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

q. If Defendant failed to provide notice of the Data Breach in a timely manner, and;

r. If Plaintiff and Class Members are entitled to damages, civil penalties, punitive

damages, treble damages, and/or injunctive relief.

112. **Typicality**. Plaintiff 's claims are typical of those of other Class Members because Plaintiff 's information, like that of every other Class Member, was compromised in the Data Breach. Moreover, Plaintiff and Class Members were subjected to Defendant's uniformly illegal and impermissible conduct.

113. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's counsel are competent and experienced in litigating complex class actions. have no interests that conflict with, or are antagonistic to, those of the Class.

114. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that Plaintiff's and Class Members' data was stored on the same computer system and unlawfully exposed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

115. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management

difficulties, conserves judicial resources, the parties' resources, and protects the rights of each Class Member.

116. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

117. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

118. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include those set forth above.

119. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

120. Plaintiff re-alleges and incorporates by reference paragraphs 1 to 132 of the Complaint as if fully set forth herein.

121. RCI required Plaintiff and Class Members to provide Defendant with Private Information to receive Defendant's products and services.

122. By collecting and storing this data in RCI's computer system and network, and

sharing it and using it for commercial gain, RCI owed a duty of care to use reasonable means to secure and safeguard its computer system—and Plaintiff's and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes so it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

123. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendant holds vast amounts of PII and PHI, it was inevitable that unauthorized individuals would at some point try to access Defendant's databases of PII and PHI.

124. After all, Private Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII and PHI of Plaintiff and Class Members. Thus, Defendant knew, or should have known, the importance of exercising reasonable care in handling the PII and PHI entrusted to Defendant.

125. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII and PHI.

126. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and Class Members, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

127. Defendant failed to take appropriate measures to protect the PII and PHI of Plaintiff and the Class. Defendant is morally culpable, given the prominence of security breaches in the healthcare industry. Any purported safeguards that Defendant had in place were wholly inadequate.

128. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff 's and the Class members' PII and PHI by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite known data breaches in the healthcare industry, and allowing unauthorized access to Plaintiff 's and the other Class Members' PII and PHI.

129. The failure of Defendant to comply with industry and federal regulations evinces Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII and PHI.

130. But for Defendant's wrongful and negligent breach of their duties to Plaintiff and the Class, Private Information would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the PII and PHI of Plaintiff and the Class and all resulting damages.

131. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff 's and the other Class members' PII and PHI. Defendant knew or should have known that their systems and technologies for processing and securing the PII and PHI of Plaintiff and the Class had security vulnerabilities.

132. As a result of this misconduct by Defendant, the PII, PHI, and other sensitive information of Plaintiff and the Classes was compromised, placing them at a greater risk of

identity theft and their PII and PHI being disclosed to third parties without the consent of Plaintiff and the Class.

133. As a direct and proximate result of RCI's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in RCI's possession and is subject to further unauthorized disclosures so long as RCI fails to undertake appropriate and adequate measures to protect the Private Information; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by RCI's data breach; (x) the value of the unauthorized access to their PII/PHI permitted by Defendant; and (xi) any nominal damages that may be awarded.

134. As a direct and proximate result of RCI's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses including nominal damages.

135. RCI's negligent conduct is ongoing, in that it still possesses Plaintiff's and Class Members' Private Information in an unsafe and insecure manner.

136. Plaintiff and Class Members are entitled to injunctive relief requiring RCI to: (i)

strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND CAUSE OF ACTION
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiff and the Nationwide Class)

137. Plaintiff re-alleges and incorporates by reference paragraphs 1 to 132 of the Complaint as if fully set forth herein.

138. Defendant entered into written contracts, including, upon information and belief, HIPAA Business Associate Agreements, with its clients to provide medication-related services.

139. In exchange, Defendant agreed, in part, to use adequate security measures to protect the Private Information of Plaintiff and the Class and to timely and adequately notify them of the Data Breach.

140. These contracts were made expressly for the benefit of Plaintiff and/or Plaintiff's dependents and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. Defendant knew that, if it were to breach these contracts with its clients, then its clients' patients— Plaintiff and Class Members—would be harmed.

141. Defendant breached the contracts it entered into with its clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiff 's Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately notify Plaintiff and Class Members of the Data Breach.

142. Plaintiff and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have

sustained as a direct and proximate result thereof.

143. Plaintiff and Class Members are also entitled to their costs and attorney's fees incurred in this action.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

144. Plaintiff re-alleges and incorporates by reference paragraphs 1 to 132 of the Complaint as if fully set forth herein.

145. Plaintiff and Class Members conferred a benefit on Defendant by entrusting their Private Information to RCI from which RCI derived profits.

146. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide adequate security.

147. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

148. Defendant acquired the PII and PHI through inequitable means in that Defendant failed to disclose the inadequate security practices, previously alleged, and failed to maintain adequate data security.

149. If Plaintiff and Class Members knew that Defendant had not secured their PII and

PHI, they would not have agreed to disclose their data to Defendant.

150. Plaintiff and Class Members have no adequate remedy at law.

151. As a direct and direct an proximate result of RCI's conduct, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in RCI's possession and is subject to further unauthorized disclosures or further entrustment to inadequate third party vendors so long as RCI fails to undertake appropriate and adequate measures to protect the Private Information; (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by RCI's data breach; (x) the value of the unauthorized access to their PII/PHI permitted by Defendant; and (xi) any nominal damages that may be awarded.

152. Plaintiff and Class Members are entitled to restitution and/or damages from RCI and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by RCI from its wrongful conduct, as well as return of their sensitive Private Information and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

153. Plaintiff and Class Members may not have an adequate remedy at law against RCI,

and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, on behalf of all others similarly situated, request the following relief:

A. An Order certifying this action as a class action and appointing Plaintiff as the Class Representative;

B. A mandatory injunction directing Defendant to adequately safeguard the PII and PHI of Plaintiff and the Class hereinafter by implementing improved security procedures and measures, including but not limited to an Order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete and purge the PII and PHI of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII and PHI;

v. requiring Defendant to engage independent third-party security auditors and internal

personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

vi. prohibiting Defendant from maintaining Plaintiff's and Class Members' PII and PHI on a cloud-based database until proper safeguards and processes are implemented;

vii. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

viii. requiring Defendant to conduct regular database scanning and securing checks;

ix. requiring Defendant to monitor ingress and egress of all network traffic;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII and PHI, as well as protecting the PII and PHI of Plaintiff and Class Members;

xi. requiring Defendant to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xii. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly

configured, tested, and updated; and

xiii. requiring Defendant to meaningfully educate all Class Members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

C. A mandatory injunction requiring that Defendant provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of PII and PHI to unauthorized persons;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII and PHI;

E. An award of damages, including actual, nominal, consequential damages, and punitive, as allowed by law in an amount to be determined;

F. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

H. Granting the Plaintiff and the Class leave to amend this Complaint to conform to the evidence produced at trial;

I. For all other Orders, findings, and determinations identified and sought in this Complaint; and

J. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Dated: December 23, 2024

Respectfully submitted,

/s/ Terence R. Coates
Terence R. Coates
Ohio Atty. Reg. No. 85579
Spencer D. Campbell*
Ohio Atty. Reg. No. 103001
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, Ohio 45202
Telephone: (513) 651-3700
Facsimile: (513) 665-0219
tcoates@msdlegal.com
scampbell@msdlegal.com

Counsel for Plaintiff and the Proposed Class

** Application for admission forthcoming*